The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/14/2020

SUBJECT:
Multiple Vulnerabilities in Apache Struts Could Allow for Remote Code Execution

OVERVIEW:
Multiple Vulnerabilities have been discovered in Apache Struts, the most severe of which could allow for remote code execution. Apache Struts is an open source framework used for building Java web applications. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
Proof of concept exploit code is available on GitHub for CVE-2019-0230.

SYSTEMS AFFECTED:
- Apache Struts versions 2.0.0 through 2.5.20

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: N/A

TECHNICAL SUMMARY:
Multiple Vulnerabilities have been discovered in Apache Struts, the most severe of which could allow for remote code execution. Details of these vulnerabilities follows:

- A vulnerability involving malicious OGNL expressions could allow for remote code execution (CVE-2019-0230)
- A vulnerability that affects the write permissions of file directories could lead to a denial of service (CVE-2019-0233)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to the most recent version of Apache Struts after appropriate testing.
- Verify no unauthorized system modifications have occurred on the system before applying the patch.
- Frequently validate type and content of uploaded data.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019:0230
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0233

Apache:
https://struts.apache.org/announce.html

GitHub:
https://github.com/A2gel/CVE-2019-0230